UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

HP computer currently located at the Portland FBI Office, 9109 NE Cascades Pkwy, Portland, Oregon, more fully described in Attachment A

Case No. 3:21-mc-00315

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

HP computer currently located at the Portland FBI Office, 9109 NE Cascades Pkwy, Portland, Oregon, more fully described in Attachment A

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. Section 2252A	Transportation, Distribution, Receiving, and Possession of Child Pornography

The application is based on these facts:

See the attached affidavit of FBI Special Agent Rebecka E. Brown.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rebecka E. Brown, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 9:41 a.m./p.m. *(specify reliable electronic means)*.

Date: March 12, 2021

Jolie A. Russo
Judge's signature

City and state: Portland, Oregon

Honorable Jolie A. Russo, U.S. Magistrate Judge
Printed name and title

STATE OF OREGON)
) ss: AFFIDAVIT OF REBECKA E. BROWN
County of Multnomah)

Affidavit in Support of an Application for a Search Warrant

I, Rebecka E. Brown, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately twelve years. I am currently assigned to the FBI's Portland Field Office. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I graduated from the FBI Academy at Quantico, Virginia, after completing a 19-week course of instruction. I have acquired knowledge and information about criminal conduct and investigation from many sources, including formal and informal training, other law enforcement officers, investigators, informants, persons who I have interviewed, and my participation in numerous investigations. I received specialized training in investigating a range of offenses from violent crime to financial crime. I have investigated matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2252A and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and Task Force Officers from Portland and Hillsboro, Oregon. The CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As part of my duties as a federal agent, I work with local, state, and other federal agencies on joint investigations of federal offenses, to include financial crimes.

//

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of the following device, which is presently in secure law enforcement custody at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland, Oregon 97220:

HP Pavilion Slimline 400 PC Series, S/N: 4C14290CLS (Device)

As set forth below, I have probable cause to believe that the Device contains the items set forth in Attachment B that constitute evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), which prohibit transporting, distributing, receiving, and possessing child pornography.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, United States Code, Section 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any

means, including by computer. Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view any material that contains child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. "Child pornography" is defined in 18 U.S.C. § 2256(8), and includes any visual depiction of a child under the age of 18 years engaged in sexually explicit conduct. "Sexually explicit conduct" is defined under 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals or pubic area of any person.

Background on Computers, Digital Devices, and Child Pornography

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

7. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited,

manipulated, copied, and distributed. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on one's person.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs and networks such as Gnutella and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

11. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in

"bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

12. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

13. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic

tools. Indeed, the very nature of the electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

Background on the BitTorrent Network

14. The BitTorrent network is a popular, publicly available P2P file sharing network. Computers that are part of that network are referred to as "peers" or "clients." Peers can download files or parts of files from other users while simultaneously providing files or parts of files to others on the network, thereby increasing downloading speed for all of the peers on the network. The BitTorrent network can be accessed through many different client software programs, including the BitTorrent client program, the uTorrent client program, the Vuze client program, and others, all of which are widely available for free on the Internet. The BitTorrent network can be accessed through a laptop or desktop computer, or through a tablet or smartphone device, such as an iPad or iPhone.

15. Files or sets of files are shared on the BitTorrent network through the use of "torrents." A torrent file is a small file that contains information about the files being shared; including information needed by the client software to locate and download the files but does not contain the files themselves. Torrent files typically contain information such as file name(s), file size(s), file paths, and an "info hash" (a digital fingerprint of sorts for the set of data referenced in the torrent file). The torrent file may also contain information on how to locate the file(s) referenced in the torrent by identifying "trackers." Trackers are computers on the BitTorrent network that collate information about peers who are sharing the files referenced in the torrent file. A tracker acts as a pointer to peers on the network who are sharing all or part of the files referenced in the torrent but does not actually have the files to be shared.

16. To locate and download files on the BitTorrent network, a user will typically enter keyword searches on a torrent indexing website. Torrent indexing websites are essentially search engines through which a BitTorrent user can locate torrent files that contain the files or type of files the user wants to download. Once the user locates a torrent file of interest, the user downloads the torrent file to his computer. The user's BitTorrent software client then uses the information in the torrent file to locate other peers on the network that have all or part of the files the user seeks and downloads the files directly from those peers. The downloaded files are then stored in the file folder or storage device designated by the user and remain there until the user moves or deletes them. Once a user downloads files (or parts of files), other users on the BitTorrent network can download those files (or parts of files) from that user, as long as the files remain in the folder/storage device designated by the user.

17. Law enforcement agents can search the BitTorrent network in much the same way in order to locate individuals who are offering to share files containing images or videos of child pornography. Law enforcement agents can search for torrents known to contain images or videos of child pornography and can download the files described in those torrents using client software designed to download only from a single source at a single IP address.

Statement of Probable Cause

Benton County Investigation of IP address 50.53.163.93

18. On Monday, March 9, 2020, Detective Christopher Dale verified that a computer running undercover investigative software located within the Benton County Sheriff`s Office, 180 NW 5th Street, Corvallis, Benton County, Oregon, made multiple direct connections to a device at IP address 50.53.163.93 between 2/14/2020 and 3/9/2020. Multiple partial and/or

complete files were successfully downloaded from the suspect device. The suspect device was the sole candidate for each download, and as such, each file was downloaded directly from the suspect device. Detective Dale reviewed several of these files and found that many contained sexually explicit conduct involving a child. Detective Dale sent the FBI an encrypted link containing files downloaded from IP address: 50.53.163.93.

FBI Investigation

19. On June 29, 2020, I reviewed the files and found them to contain child pornography (CP). Descriptions of two files follow:

File:..\Download\AG-132\[Kinderkutje]Build-10Yo-11Yo.mpg

Date: March 9, 2020 at 13:01 (UTC)

Description: A 4m24s montage of videos depicting prepubescent and pubescent females, aged ten to twelve years old, graphically and sexually displaying their vaginal areas. Various sections of the video depict prepubescent girls, some nude, some partially clothed, in a variety of poses with a focus on their exposed genitals. Some video segments show girls inserting fingers into their vaginas as someone films.

File:..\Download\(Kinderkutje) Jenny 9Yo All Cllips 01.avi

Date: March 5, 2020 at 06:16 (UTC)

Description: An approximately 39 second video of a four to five year old girl wearing a pink Winnie the Pooh shirt sitting on a bed. A nude adult male with an erect penis is standing in front of her. The adult male instructs the girl to hold his

penis, which she does, before he moves aside to adjust the camera. When the man returns, he tells the girl to look at the camera while she licks his penis.

20. On July 17, 2020, the FBI issued a subpoena to Ziply Fiber for subscriber information associated with the following IP address: 50.53.163.93 on 03/09/2020 at 13:01 UTC. On July 22, 2020, Northwest Fiber Communications (Ziply Fiber) responded to the request advising that for subscriber information before May 1, 2020, in Washington, Oregon, Idaho, and Montana, Frontier Communications should be contacted. Ziply Fiber does not maintain records prior to this date.

21. On July 22, 2020, the FBI issued a subpoena to Frontier Communications for subscriber information associated with the following IP address: 50.53.163.93 on 03/09/2020 at 13:01 UTC. On July 29, 2020, Frontier Communications responded with the following subscriber information:

Customer Name: Robert Kyle

Account Address: 3549 16th Place, Forest Grove, OR

22. On July 30, 2020, at approximately 10:05 A.M., a physical surveillance was conducted at 3549 16th Place, Forest Grove, Oregon. The residence is a single-story detached house painted a light blue-gray with a light gray composite roof. The numbers, "3549" were affixed to the right of the garage door. The white front door was covered by a white storm door. A late model white Ford F-150 pickup bearing Oregon license plate 807LZJ was parked on the street in front of the residence. A maroon-colored Ford Fiesta bearing Oregon license plate 676FCG was parked in the driveway. According to the Oregon Department of Motor Vehicles,

the above vehicles were registered to Robert Dean KYLE and his wife at 3549 16th Place, Forest Grove, Oregon.

23. A WiFi survey taken directly in front of the residence revealed that all visible SSID's were encrypted/password protected.

24. On August 3, 2020, an NCIC query for Robert KYLE resulted in no identifiable criminal history.

25. On February 24, 2021, an FBI Task Force Officer and I interviewed Robert KYLE at his residence regarding the activity observed on his IP address in February and March 2020. KYLE admitted that he used a Microsoft-based computer in his house to access the BitTorrent network to download movies and pornography, including child pornography. KYLE further stated that files depicting CP could still be found on the computer. KYLE was advised that since law enforcement was aware that files that were illegal to possess were currently on a computer in his house, he would have to surrender the device. KYLE was told that he could voluntarily do this, or law enforcement could seize his house and apply for a search warrant. Either way, investigators would seek a search warrant from a magistrate judge to examine his computer. KYLE stated that he understood and agreed to surrender his computer, an HP Pavilion Slimline 400 PC Series, the Device, which is further described in Attachment A. At the conclusion of the interview, KYLE was asked if child modeling images would be found on his computer, to which he replied, "Oh, worse than that."

26. I brought the Device back to the FBI office in Portland, Oregon, and entered in as evidence. The Device is being held in secure storage.

//

Examination of Data Storage Devices

27. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

28. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, is often essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

29. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications

do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

30. *Latent Data*: Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file.

31. *Contextual Data*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and

the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital

device. Specifically, the lack of computer security software, virus protection, and malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

32. In searching the Device, law enforcement personnel executing the search warrant will employ the following procedure:

a. Because the Device to be searched is already in law enforcement custody, it will be transported to an appropriate law enforcement laboratory for review.

b. Law enforcement personnel will examine the Device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g. evidence of other crimes), they will seek an additional warrant.

c. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

d. Law enforcement personnel will perform an initial search of the Device within a reasonable amount of time not to exceed 120 days from the date of the execution of the warrant. If the government needs additional time to determine whether the Device contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant. The government shall complete the search of the Devices within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

e. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on the Device do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files,

registry data, and the like), through the conclusion of the case.

f. If the Device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return the Device to its owner within a reasonable period of time following the search of the Device, and will seal any image of the Device, absent further authorization from the Court.

g. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

Data to be Seized

33. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. The Device, presently in secure evidence storage at the Portland FBI office, for contraband or the types of evidence, fruits, or instrumentalities of the crimes of transporting, distributing, receiving, and possessing child pornography, as set forth in Attachment B, including;

1. All records on the Device that relate to violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B), including:

a. Evidence of any Peer-to-Peer software, including date and time of installation, usage, and file sharing;

b. Evidence of Internet usage for the transportation, receipt, distribution, or possession of child pornography as defined in 18 U.S.C.

§ 2256, including dates and times of usage; IP addresses; and user names and passwords used to access the Internet or any accounts via the Internet;

c. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including all motion pictures or digital video clips containing such visual depictions;

d. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

e. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

f. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined

in 18 U.S.C. § 2256;

h. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

i. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

j. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed; and

k. Storage media used as a means to commit or facilitate the violations described above.

2. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the Device or data;

3. Any passwords, password files, test keys, encryption codes, or other information necessary to access the Device or data;

4. Any evidence of user attribution showing who used or owned the Device at the time the things described in Attachment B were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

5. Any records evidencing the use of the Internet using the Device, including:

a. Records of IP addresses used;

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

c. Records of data storage accounts and use of data storage accounts.

34. The government has made no prior efforts in other judicial fora to obtain the evidence sought in this warrant.

Retention of Image

35. The government will retain a forensic image of the electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

36. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the

physical storage media that were seized or imaged.

Conclusion

37. Based on the foregoing, I have probable cause to believe that the device described in Attachment A, contains evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

38. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorneys (AUSA) Natalie Wight and Andrew Ho prior to being submitted to the Court. AUSAs Wight and Ho advised me that in their opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

REBECKA E. BROWN
Special Agent
Federal Bureau of Investigation

Sworn via telephone pursuant to Fed. R. Crim. P. 4.1 at 9:41 [A.M./P.M.] this 12 day of March, 2021.

Jolie A. Russo

THE HONORABLE JOLIE A. RUSSO
United States Magistrate Judge

ATTACHMENT A

Items to be Searched

The following digital device, which was seized from Robert Dean KYLE on February 24, 2021, and is currently in secure evidence storage at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland, Oregon 97220:

HP Pavilion Slimline 400 PC Series, S/N: 4C14290CLS

ATTACHMENT B

Items to Be Seized

1. All records on the device described in Attachment A (Device) that relate to violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B) (transportation, receipt, distribution, and possession of child pornography), including:

a. Evidence of any Peer-to-Peer software, including date and time of installation, usage, and file sharing;

b. Evidence of Internet usage for the transportation, receipt, distribution, or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage; IP addresses; and user names and passwords used to access the Internet or any accounts via the Internet;

c. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including all motion pictures or digital video clips containing such visual depictions;

d. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

e. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

f. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

h. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

i. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

j. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed; and

k. Storage media used as a means to commit or facilitate the violations described above.

2. Physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the Device, storage devices, or data.

3. Passwords, password files, test keys, encryption codes, or other information necessary to access the Device, storage devices, or data.

4. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

5. Records evidencing the use of the Internet, including:

a. Records of IP addresses used;

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

c. Records of data storage accounts and use of data storage accounts.

6. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

7. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

8. The initial examination of the Device will be performed within a reasonable

amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

9. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

10. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to the owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

11. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

12. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to

questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.